

FORM PTO-1390 (Modified) (REV 11-98)		U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE		ATTORNEY'S DOCKET NUMBER	
TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371				1235-00	
INTERNATIONAL APPLICATION NO. PCT/US00/26828		INTERNATIONAL FILING DATE 29 SEP 00		U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR 09/701261	
				PRIORITY DATE CLAIMED 01 OCT 99	
TITLE OF INVENTION METHOD & SYSTEM FOR PROVIDING DATA SECURITY IN A FILE SYSTEM MONITOR WITH STACK POSITIONING					
APPLICANT(S) FOR DO/EO/US FRIEDMAN, George; STAREK, Robert Phillip; MURDOCK, Carlos A.					
Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:					
<ol style="list-style-type: none"> <input checked="" type="checkbox"/> This is a FIRST submission of items concerning a filing under 35 U.S.C. 371. <input type="checkbox"/> This is a SECOND or SUBSEQUENT submission of items concerning a filing under 35 U.S.C. 371. <input checked="" type="checkbox"/> This is an express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1). <input type="checkbox"/> A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date. <input checked="" type="checkbox"/> A copy of the International Application as filed (35 U.S.C. 371 (c) (2)) <ul style="list-style-type: none"> <input type="checkbox"/> is transmitted herewith (required only if not transmitted by the International Bureau). <input type="checkbox"/> has been transmitted by the International Bureau. <input checked="" type="checkbox"/> is not required, as the application was filed in the United States Receiving Office (RO/US). <input type="checkbox"/> A translation of the International Application into English (35 U.S.C. 371(c)(2)). <input type="checkbox"/> A copy of the International Search Report (PCT/ISA/210). <input type="checkbox"/> Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371 (c)(3)) <ul style="list-style-type: none"> <input type="checkbox"/> are transmitted herewith (required only if not transmitted by the International Bureau). <input type="checkbox"/> have been transmitted by the International Bureau. <input type="checkbox"/> have not been made; however, the time limit for making such amendments has NOT expired. <input type="checkbox"/> have not been made and will not be made. <input type="checkbox"/> A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)). <input checked="" type="checkbox"/> An oath or declaration of the inventor(s) (35 U.S.C. 371 (c)(4)). <input type="checkbox"/> A copy of the International Preliminary Examination Report (PCT/IPEA/409). <input type="checkbox"/> A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371 (c)(5)). 					
Items 13 to 20 below concern document(s) or information included:					
<ol style="list-style-type: none"> <input type="checkbox"/> An Information Disclosure Statement under 37 CFR 1.97 and 1.98. <input checked="" type="checkbox"/> An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included. <input type="checkbox"/> A FIRST preliminary amendment. <input type="checkbox"/> A SECOND or SUBSEQUENT preliminary amendment. <input type="checkbox"/> A substitute specification. <input type="checkbox"/> A change of power of attorney and/or address letter. <input checked="" type="checkbox"/> Certificate of Mailing by Express Mail <input type="checkbox"/> Other items or information: 					
<input type="checkbox"/> Acknowledgement postcard 					

U.S. APPLICATION NO. (IF KNOWN) SEE 37 CFR 09/701201		INTERNATIONAL APPLICATION NO. PCT/US00/26828	ATTORNEY'S DOCKET NUMBER 1235-00																				
21. The following fees are submitted:		CALCULATIONS PTO USE ONLY																					
BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)) : <ul style="list-style-type: none"> <input type="checkbox"/> Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2) paid to USPTO and International Search Report not prepared by the EPO or JPO \$1,000.00 <input type="checkbox"/> International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO \$860.00 <input checked="" type="checkbox"/> International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO \$710.00 <input type="checkbox"/> International preliminary examination fee paid to USPTO (37 CFR 1.482) but all claims did not satisfy provisions of PCT Article 33(1)-(4) \$690.00 <input type="checkbox"/> International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(1)-(4) \$100.00 																							
ENTER APPROPRIATE BASIC FEE AMOUNT =		\$710.00																					
Surcharge of \$130.00 for furnishing the oath or declaration later than months from the earliest claimed priority date (37 CFR 1.492 (e)).		<input type="checkbox"/> 20 <input type="checkbox"/> 30	\$0.00																				
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>CLAIMS</th> <th>NUMBER FILED</th> <th>NUMBER EXTRA</th> <th>RATE</th> </tr> </thead> <tbody> <tr> <td>Total claims</td> <td>32 - 20 =</td> <td>12</td> <td>x \$18.00 \$216.00</td> </tr> <tr> <td>Independent claims</td> <td>4 - 3 =</td> <td>1</td> <td>x \$80.00 \$80.00</td> </tr> <tr> <td colspan="2">Multiple Dependent Claims (check if applicable).</td> <td colspan="2" style="text-align: right;"><input type="checkbox"/></td> </tr> <tr> <td colspan="2" style="text-align: center;">TOTAL OF ABOVE CALCULATIONS =</td> <td colspan="2" style="text-align: right;">\$1,006.00</td> </tr> </tbody> </table>		CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE	Total claims	32 - 20 =	12	x \$18.00 \$216.00	Independent claims	4 - 3 =	1	x \$80.00 \$80.00	Multiple Dependent Claims (check if applicable).		<input type="checkbox"/>		TOTAL OF ABOVE CALCULATIONS =		\$1,006.00			
CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE																				
Total claims	32 - 20 =	12	x \$18.00 \$216.00																				
Independent claims	4 - 3 =	1	x \$80.00 \$80.00																				
Multiple Dependent Claims (check if applicable).		<input type="checkbox"/>																					
TOTAL OF ABOVE CALCULATIONS =		\$1,006.00																					
Reduction of 1/2 for filing by small entity, if applicable. Verified Small Entity Statement must also be filed (Note 37 CFR 1.9, 1.27, 1.28) (check if applicable).		<input type="checkbox"/>		\$0.00																			
		SUBTOTAL =		\$1,006.00																			
Processing fee of \$130.00 for furnishing the English translation later than months from the earliest claimed priority date (37 CFR 1.492 (f)).		<input type="checkbox"/> 20 <input type="checkbox"/> 30	+	\$0.00																			
		TOTAL NATIONAL FEE =		\$1,006.00																			
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31) (check if applicable).		<input checked="" type="checkbox"/>		\$40.00																			
		TOTAL FEES ENCLOSED =		\$1,046.00																			
<input type="checkbox"/> A check in the amount of \$1,046.00 to cover the above fees is enclosed.				Amount to be: refunded \$																			
<input type="checkbox"/> Please charge my Deposit Account No. 13-3405 in the amount of A duplicate copy of this sheet is enclosed.				charged \$																			
<input checked="" type="checkbox"/> The Commissioner is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. 13-3405 A duplicate copy of this sheet is enclosed.																							
NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.																							
SEND ALL CORRESPONDENCE TO:																							
PAUL A. TAUFER, ESQ. SCHNADER HARRISON SEGAL & LEWIS, LLP 1600 MARKET STREET, SUITE 3600 PHILADELPHIA, PA 19103 (215) 751-2475 (215) 568-6946 - fax		 SIGNATURE <hr/> Paul A. Taufer <hr/> NAME <hr/> 35,703 <hr/> REGISTRATION NUMBER <hr/> November 27, 2000 <hr/> DATE																					

METHOD AND SYSTEM FOR PROVIDING DATA SECURITY
IN A FILE SYSTEM MONITOR WITH STACK POSITIONING

Field of the Invention

5 The present invention pertains to the field of file systems in electronic computers. In particular, the invention relates to a method and system for providing data security in a file system monitor using stack positioning.

Background of the Invention

10 Computer systems typically include one or more local or networked data storage devices. A typical application program executing on such a computer system accesses such data storage devices by calling standard file system services provided by an operating system, such as services for creating, reading, and writing files on the data storage devices.

15 A device driver is a set of computer-implemented instructions that implements the device-specific aspects of generic input/output operations. In typical operating systems, software applications such as device drivers run in either "kernel mode" or "user mode." A virtual device driver is a type of device driver that has direct access to an operating system kernel, such as by running in kernel mode. "Kernel mode" is a highly privileged memory access mode of the processor. "User mode" is a less privileged memory access mode of the processor. The memory 20 access mode is a part of the hardware state of the processor. The kernel mode privilege level is also known as "Ring 0," and the user mode privilege level is also known as "Ring 3." Kernel mode access allows the virtual device driver to interact with system and hardware resources at a very low level.

In conventional operating systems, device drivers may be represented as layered on top of 25 one another. The layered architecture is also sometimes referred to as a stack or a calling chain. It is the lowest-level device driver that typically controls a hardware device. If there is only a single device driver above the hardware device, the driver is called a monolithic driver. However, a plurality of drivers may be placed above the lowest-level driver. Input and output requests ("I/O requests") to the hardware device or devices controlled by a lowest-level driver are 30 handled first by the highest-level driver, then seriatim by any lower-level intermediate drivers, and finally by the lowest-level driver.

A file system driver is generally a highest-level driver, layered above a device driver for a data storage device such as a hard disk drive. The file system driver implements high-level

aspects of I/O requests directed to the file system, such as requests to create, open, extend, and delete files and directories. A plurality of file system drivers may exist in a single computer, and file system drivers may be specific to different types of file systems, such as the FAT and NTFS file systems.

- 5 It is known in the art to monitor file I/O requests in operating systems having an installable file system manager and layered device drivers, such as the Windows 95®, Windows 98®, and Windows Me® operating systems available from Microsoft Corporation of Redmond, Washington, and collectively referred to herein as "Windows 9x". In Windows 9x operating systems, file system monitoring may be accomplished by registering a file system applications
10 programming interface hook with the installable file system manager. Windows 9x provides a function called IFSMGR_InstallFileSystemApiHook which is designed to be used for monitoring I/O requests to a file system. This service allows virtual device drivers to monitor all file system activity by hooking into the file system calls. By means of a call during system initialization to IFSMGR_InstallFileSystemApiHook, a virtual device driver may insert itself onto the stack of all
15 file system requests.

A somewhat different approach has been used to monitor file systems on object-oriented operating systems, such as the Windows NT® operating system and successor operating systems such as Windows 2000®, available from Microsoft Corporation of Redmond, Washington, and collectively referred to herein as "Windows NT." In Windows NT, I/O requests are described by
20 data structures known as I/O Request Packets ("IRPs"), which are used for communication between software applications and drivers. All IRPs to hardware devices are handled by device drivers operating in kernel mode. High-level, intermediate, and low-level drivers exchange IRPs to complete a given I/O request. The lowest-level driver calls an NT layer known as the Hardware Access Layer (HAL) to gain direct control of the hardware. It is known on a Windows
25 NT system to implement a file system monitor as a device driver object that creates filter device objects and attaches those objects to target file system device objects, so that the file system monitor will see all IRPs directed to the monitored data storage devices.

There is a need in the field of file systems in electronic computers to prevent unauthorized activity. Unauthorized activity includes, without limitation, the release of data
30 from a secured file or a secured file system to an insecure file system device driver, and the malicious, unauthorized, or accidental modification or corruption of data, such as by computer viruses. Conventional file system drivers, such as file system monitors that are used to detect and monitor activity in file systems, have not typically included effective security measures to

prevent unauthorized activity by a software application or device driver that is layered, or attempts to layer itself, at a higher level than the highest-level device driver above the targeted data storage device.

5 **Summary of the Invention**

It is a principal object of the present invention to improve the security of data stored in data storage devices on electronic computers.

Another object of the present invention is to prevent unauthorized activity in connection with secured data files or file systems.

10 Another object of the present invention is to maintain the position of the device driver of the present invention as the highest-level device driver above a secured data storage device.

Another object of the present invention is to prevent any software application or device driver from being layered at a higher level than the device driver of the present invention, and thereby gaining access that would permit unauthorized activity.

15 These and other objects are provided by a method and system for providing data security in a file system monitor by stack positioning.

More particularly, the present invention relates to a method for providing data security in a first device driver operably installed in a computer operating system having a layered plurality of device drivers for accessing data in a data storage device, comprising the steps of detecting an

20 I/O request, and determining whether the first device driver is functionally uppermost in the layered plurality of device drivers. If the first device driver is functionally uppermost in the layered plurality of device drivers, the method of the invention performs the I/O request in the first device driver. If the first device driver is not functionally uppermost in the layered plurality of device drivers, the method of the invention denies the I/O request in the first device driver,

25 and allows the I/O request to be performed by a next lower-level device driver in the layered plurality of device drivers.

In another aspect, the invention relates to a system for providing data security, the system comprising a first device driver operably installed in a computer operating system having a layered plurality of device drivers for accessing data in a data storage device.

30 In still another aspect, the invention comprises a machine-readable medium comprising secured data and a first device driver program for providing data security when operably installed in a computer operating system having a layered plurality of device drivers for accessing data in a data storage device.

In yet another aspect, the invention comprises a computer-implemented first device driver for providing data security when operably installed in a computer operating system having a layered plurality of device drivers for accessing data in a data storage device.

Further objects and advantages of this invention will become apparent from the detailed

5 description of a preferred embodiment, which follows.

Brief Description of the Drawings

The present invention is described in further detail with reference to the accompanying drawings. The figures of the accompanying drawings illustrate the present invention by way of 10 example and not limitation.

FIG. 1 is a diagram of the system architecture layout of the Windows 9x operating system.

FIG. 2 is a diagram of the system architecture layout of the Windows NT operating system.

15 FIG. 3 is a flow chart illustrating an embodiment of the stack positioning method of the present invention.

FIG. 4 is a flow chart illustrating the re-hooking steps of the stack positioning method of the present invention.

Detailed Description of Preferred Embodiments of the Invention

The invention will be understood more fully from the detailed description given below; which, however, should not be taken to limit the invention to a specific embodiment, but is for explanation and understanding only.

The terms "computer" or "computer system," as used herein, include any device capable 25 of receiving, transmitting, and/or using information, including, without limitation, a processor; a microprocessor; a personal computer, such as a laptop, palm PC, desktop or workstation; a network server; a mainframe; an electronic wired or wireless device, such as for example, a telephone; an interactive television or electronic box attached to a television, such as for example, a television adapted to be connected to the Internet; a cellular telephone; a personal 30 digital assistant; an electronic pager; and a digital watch. In an illustrative example, information is transmitted in the form of e-mail. A computer, computer system, or system of the invention may operate in communication with other systems over a network, such as, for example, the Internet, an intranet, or an extranet, or may operate as a stand-alone system.

It should also be understood that the terms "device driver" or "driver," as used herein, include any computer-implemented instructions for directly or indirectly accessing or controlling hardware devices, including, without limitation, device drivers, virtual device drivers (VxDs), instructions using NT kernel mode architecture, instructions using Win32 driver model (WDM),
5 and other instructions, in any computer language, directed to any computer, computer architecture, network, or operating system.

Although the embodiment illustrated in the figures comprises a device driver described for illustrative purposes as a "file system monitor," the term "file system monitor" as used herein refers generally to a device driver of any kind using the stack positioning of the present
10 invention. Device drivers within the scope of the invention may perform any sort of useful function that may be performed by a device driver, including, without limitation, general-purpose monitoring, permission monitoring, filtering, encryption, decryption, virus detection, data mirroring, I/O functions directed toward any device, and other functions, and are not limited to either monitoring or to functions related to file systems. Any device driver which accomplishes
15 stack positioning appropriately falls within the scope of the present invention.

One embodiment of the present invention may be implemented on a Windows 9x operating system. Referring now to FIG. 1, components of the Windows 9x operating system are divided between user mode code 10 and kernel mode code 30, which provide different levels of system protection. For one embodiment, the user mode code 10 includes a system virtual
20 machine 20 capable of running 16-bit and 32-bit software applications 21-22, and a plurality of MS-DOS virtual machines 25. In this embodiment, the kernel mode code 30 comprises low-level operating system services and virtual device drivers, such as a virtual machine manager 40, a file system monitor 50 of the present invention, and an installable file system manager 60.

Beneath the installable file system manager 60 are a plurality of file system drivers 70-72
25 for file systems such as FAT and NTFS. Beneath the file system drivers 70-72 is a block I/O subsystem 80. The block I/O subsystem 80 includes an I/O supervisor 81 which manages requests as they pass through the file system hierarchy, a monolithic driver 82 for port I/O, and a layered plurality of device drivers 83-84.

In this embodiment, the first device driver 50 intercepts all I/O requests from user mode
30 code 10 and from applications 21-22 running in user mode 10, before the I/O requests are sent to the installable file system manager 60. The first device driver 50 is able to monitor and, if desired, filter all file system activity occurring in the installable file system manager 60, file system drivers 70-72, and block I/O subsystem 80. By means of a call during system

initialization to IFSMGR_InstallFileSystemApiHook, the first device driver 50 is hooked into such calls when the operating system is started or restarted, at which time it is inserted into a functionally uppermost position on the stack of all file system requests. From the installable file system manager 60 down through each driver in the layered plurality 83-84, an I/O request is
5 passed from the highest level to the lowest level, and the devices can also view the result of a request as it passes back up the stack to the source of the I/O request. Each device driver on the stack may service an I/O request itself and not pass the I/O request to lower levels, or may, if desired, itself generate a new I/O request. Such device drivers may implement functions that require waiting, such as for an interrupt, or for a device to become available. During such
10 waiting periods the device driver simply returns to its caller, allowing the calling application or device driver to perform other work in parallel with the I/O request. In the alternative, the calling application or device driver can simply wait ("block") until the I/O request is complete.

In another embodiment, illustrated with reference to FIG. 2, the present invention may be implemented on a Windows NT operating system. As is well known in the art, an application
15 100 running in user mode under Windows NT may send an I/O request to operating system services 110. I/O manager 120 receives I/O requests, and coordinates the transfer of I/O request packets among various drivers. In the alternative, the various drivers may communicate directly with each other without using an I/O manager 120 or other device to coordinate transfer of information among the various drivers.

The conventional input/output system of operating systems such as Windows NT comprises a plurality of device drivers 130-132 for processing I/O requests. Such device drivers are illustrated, for example, by file system drivers 130, and a layered plurality of device drivers 131-132. The I/O manager 120 typically delivers I/O request packets to the file system driver 130 responsible for managing the target of the I/O request. However, as is known in the art, a
25 file system monitor 50 can attach to other device drivers 130-132 in an object-oriented fashion. Thereupon, the I/O manager 120 routes I/O request packets intended for the target device driver 130-132 to the file system monitor 50 that has attached to the target device driver 130-132. In this illustrative embodiment, the file system monitor 50 attaches to each of the plurality of file system driver objects 130.

FIG. 3 is a flow chart of one embodiment of a method for providing data security in a file system monitor 50 using stack positioning. For illustrative purposes, an embodiment is shown in which the file system monitor 50 filters file system requests, which are I/O requests directed to a file system. It should be understood, however, that the present invention may be usefully

implemented in any device driver, regardless of the purpose of such device driver, without regard to file systems or monitoring functions.

As shown in FIG. 3, the stack positioning process of the present invention is initiated, in step 200, each time a file system request is detected. In step 210, the process determines whether 5 or not the file system filter has been shut down by a previous iteration of step 223. If so, the process continues at step 225, allowing subsequent calls to go unfiltered, and exits at step 233.

Returning to step 210, if the file system filter has not been previously shut down, the process continues at step 220 and determines whether this is the first file system request detected by step 200.

10 If so, the process continues at step 230 and determines the calling module address. Because this is the first file system request, it is logically guaranteed that the file system monitor 50 has just been loaded, and therefore is functionally uppermost in the stack of device drivers relating to the file system. In a Windows NT embodiment, the calling module is determined by reference to an attached device field of the file system monitor 50, which will be zero when the 15 file system monitor 50 is functionally uppermost in the stack of device drivers. Continuing to step 231, the process stores the calling module address determined at step 230. The process continues at step 232 and completes the filtering functions or other useful functions implemented in file system monitor 50. The process then concludes at step 233.

20 Returning to step 220, if this is not the first file system request detected by step 200, the process continues at step 221 and determines the calling module address. In a Windows NT embodiment, the calling module is determined by reference to an attached device field of the file system monitor 50, which will be non-zero if any device object has attached to the file system monitor 50. At step 222, the calling module address is compared to the address that was 25 previously stored at step 231. By comparing the calling module addresses at this point, the file system monitor 50 will be able to detect any other driver which attempts to obtain priority over the file system monitor 50 by interposing itself between the calling module and the file system monitor 50. If the two calling module addresses are the same at step 222, the process continues at step 232.

If the two calling module addresses are not the same at step 222, the process continues at 30 step 223, and sets a flag indicating shutdown of filtering. This flag is the same flag that is checked at step 210. The process continues at step 224 and initiates the re-hook process, which is described below with reference to FIG. 4. After step 224, the process continues at step 225, allowing subsequent calls to go unfiltered, and exits at step 233.

FIG. 4 is a flow chart of one embodiment of a re-hook process. At step 300, the re-hook process of the present invention is initiated. Continuing to step 310, the process increments a stored count of how many times the re-hook process has been started. Continuing to step 320, the process determines whether the stored count has reached a maximum threshold. The

- 5 maximum threshold is a predetermined value which triggers a programmable security response.

In embodiments where there is zero tolerance for attempts to circumvent data security, a maximum threshold value of one will be appropriate. In embodiments where some tolerance is acceptable, a maximum threshold value higher than one will be appropriate. In alternate embodiments, multiple or alternative programmable security responses may be enabled at
10 different thresholds.

A wide range of programmable security responses may be found desirable.

Programmable security responses include, without limitation, destroying the data that was requested, or, if such data is stored in a secure virtual file system, destroying both the data and the secure virtual file system. Further embodiments of programmable security responses include terminating open applications, destroying the file system monitor on the data storage device, halting the operation of the computer, and causing the computer to enter a state requiring reboot. The preceding are illustrative examples only, and should not be construed to limit the variety of programmable security responses according to the present invention.

- Returning to step 320, if the stored count has reached the maximum threshold, at step
20 330, the programmable security response is initiated, and the process concludes at step 350.

If the stored count has not reached the maximum threshold, at step 340 the process initiates reattachment of the file system monitor 50. This may be accomplished by initializing a new file system monitor 50 at the functionally uppermost level in the stack. In an object-oriented environment such as Windows NT, there may be many attachments to a single device object, and
25 it is not necessary to remove or detach the file system monitor 50 from the stack, although it may be desirable to do so. Reattachment may, in an alternate embodiment, be accomplished by editing the calling chain to return the previously initialized file system monitor 50 to the functionally uppermost level.

At step 340, the process also unsets the flag indicating shutdown of filtering, to indicate
30 that filtering may be resumed. This flag is the same flag, with reference to FIG. 3, that is set at step 223 and checked at step 210. The process then concludes at step 350.

What have been described are only some examples of methods and systems according to the invention. Various modifications to the preferred embodiments will be readily apparent to

those skilled in the art, and the generic principles defined herein may be applied to other embodiments and applications without departing from the spirit and scope of the invention. Thus, the present invention is not intended to be limited to the embodiments shown. On the contrary, it is to be understood that various and numerous other arrangements may be devised by one skilled in the art without departing from the spirit and scope of the invention as limited only by the accompanying claims.

We claim:

1. A method for providing data security in a first device driver operably installed in a computer operating system having a layered plurality of device drivers for accessing data in a
5 data storage device, the method comprising the steps of:

detecting an I/O request to said first device driver;

10 determining whether said first device driver is functionally uppermost in the layered plurality of device drivers;

if said first device driver is functionally uppermost in the layered plurality of device drivers, performing the I/O request in said first device driver; and

15 if said first device driver is not functionally uppermost in the layered plurality of device drivers, denying the I/O request in said first device driver, and allowing the I/O request to be performed by a next lower-level device driver in the layered plurality of device drivers.

- 20 2. The method of claim 1 wherein said first device driver is a file system monitor.

- 25 3. The method of claim 1 wherein the data is stored in a secure virtual file system, and wherein the step of performing the I/O request further comprises the step of implementing data security measures.

- 30 4. The method of claim 1 wherein the data is stored in encrypted form, and wherein the step of performing the I/O request further comprises the step of decrypting the data.

5. The method of claim 1 wherein the step of performing the I/O request further comprises the step of checking the data for viruses.

- 35 6. The method of claim 1 wherein the step of determining whether said first device driver is functionally uppermost in the layered plurality of device drivers further comprises the steps of:

determining whether said first device driver has been previously called;
if said first device driver has not been previously called, detecting an initial calling module address, storing said initial calling module address, and concluding that said first device driver is functionally uppermost in the layered plurality of device drivers;

5 if said first device driver has been previously called, detecting a second calling module address, comparing said second calling module address to the initial calling module address, and concluding that said first device driver is functionally uppermost in the
10 layered plurality of device drivers only if the initial calling module address matches the second calling module address.

7. The method of claim 1 wherein the step of denying the I/O request in the secure first device driver comprises the steps of:

15 setting a first device driver shutdown flag; and

initiating a re-hook process.

20 8. The method of claim 1 further comprising, after the step of detecting an I/O request to said first device driver, the steps of:

25 checking whether a first device driver shutdown flag is set; and

if said first device driver shutdown flag is set, omitting further steps in said first device driver, and allowing the I/O request to be performed by a next lower-level device driver in the layered plurality of device drivers.

30 9. The method of claim 7 wherein the step of initiating a re-hook process further comprises the steps of:

counting the number of times the re-hook process has been initiated;

checking whether the number of times has reached a predetermined maximum threshold;

if the number of times has reached a predetermined maximum threshold, initiating a programmable security response;

5

if the number of times has not reached a predetermined maximum threshold, initiating reattachment of said first device driver functionally uppermost in the layered plurality of device drivers;

10

if said first device driver has been reattached functionally uppermost in the layered plurality of device drivers, unsetting said first device driver shutdown flag; and

concluding the re-hook process.

15

10. The method of claim 9 wherein the programmable security response comprises the step of destroying the data.

15

11. The method of claim 9 wherein the data is stored in a secure virtual file system, and wherein the step of destroying the data further comprises the step of destroying the secure virtual 20 file system.

20

12. The method of claim 9 wherein the programmable security response comprises the step of terminating open applications.

25

13. The method of claim 9 wherein the programmable security response comprises the step of destroying said first device driver on the data storage device.

30

14. The method of claim 9 wherein the programmable security response comprises the step of halting the operation of the computer.

15. The method of claim 9 wherein the programmable security response comprises the step of causing the computer to enter a state requiring reboot.

16. A system for providing data security, the system comprising a first device driver operably installed in a computer operating system having a layered plurality of device drivers for accessing data in a data storage device, wherein said first device driver:

5 detects an I/O request;

determines whether said first device driver is functionally uppermost in the layered plurality of device drivers;

10 if said first device driver is functionally uppermost in the layered plurality of device drivers, performs the I/O request; and

15 if said first device driver is not functionally uppermost in the layered plurality of device drivers, denies the I/O request, and allows the I/O request to be performed by a next lower-level device driver in the layered plurality of device drivers.

20 17. The method of claim 16 wherein said first device driver is a file system monitor.

25 18. The system of claim 16 further comprising a secure virtual file system for storing the data, and wherein said first device driver performs the I/O request by implementing data security measures.

30 19. The system of claim 16 wherein the data is stored in encrypted form, and wherein said first device driver performs the I/O request by decrypting the data.

25 20. The system of claim 16 wherein said first device driver performs the I/O request by checking the data for viruses.

30 21. The system of claim 16 wherein said first device driver determines whether it is functionally uppermost in the layered plurality of device drivers by:

 determining whether said first device driver has been previously called;

if said first device driver has not been previously called, detecting an initial calling module address, storing said initial calling module address, and concluding that said first device driver is functionally uppermost in the layered plurality of device drivers;

- 5 if said first device driver has been previously called, detecting a second calling module address, comparing said second calling module address to the initial calling module address, and concluding that said first device driver is functionally uppermost in the layered plurality of device drivers only if the initial calling module address matches the second calling module address.

10

22. The system of claim 16 further comprising a first device driver shutdown flag and a re-hook system, wherein said first device driver denies the I/O request by setting a first device driver shutdown flag and calling the re-hook system.

15

23. The system of claim 16 further comprising a first device driver shutdown flag, wherein, after said first device driver detects an I/O request, said first device driver:

checks whether a first device driver shutdown flag is set; and

20

if said first device driver shutdown flag is set, omits further steps in said first device driver, and allows the I/O request to be performed by a next lower-level device driver in the layered plurality of device drivers.

25

24. The system of claim 22 wherein the re-hook system further comprises a counter that counts the number of times the re-hook system has been initiated, and wherein the re-hook system:

checks whether the number of times has reached a predetermined maximum threshold;

30

if the number of times has reached a predetermined maximum threshold, initiates a programmable security response;

if the number of times has not reached a predetermined maximum threshold, initiates

reattachment of said first device driver functionally uppermost in the layered plurality of device drivers; and

if said first device driver has been reattached functionally uppermost in the layered plurality of device drivers, unsets said first device driver shutdown flag.

5 25. The system of claim 24 wherein the programmable security response destroys the data.

10 26. The system of claim 24 further comprising a secure virtual file system for storing the data, and wherein the programmable security response destroys the data and destroys the secure virtual file system.

15 27. The system of claim 24 wherein the programmable security response terminates open applications.

28. The system of claim 24 wherein the programmable security response destroys said first device driver on the data storage device.

20 29. The system of claim 24 wherein the programmable security response halts the operation of the computer.

30. The system of claim 24 wherein the programmable security response causes the computer to enter a state requiring reboot.

25 31. A machine-readable medium comprising secured data and a first device driver program for providing data security when operably installed in a computer operating system having a layered plurality of device drivers for accessing data in a data storage device, said first device driver program comprising:

30 computer-implemented instructions for detecting an I/O request to said first device driver;

computer-implemented instructions for determining whether said first device driver is functionally uppermost in the layered plurality of device drivers;

computer-implemented instructions for performing the I/O request in said first device driver if said first device driver is functionally uppermost in the layered plurality of device drivers; and

5 computer-implemented instructions for denying the I/O request in said first device driver if said first device driver is not functionally uppermost in the layered plurality of device drivers, and for allowing the I/O request to be performed by a next lower-level device driver in the layered plurality of device drivers if said first device driver is not functionally uppermost in the layered plurality of device drivers.

PCT/US00/26827

10 32. A computer-implemented first device driver for providing data security when operably installed in a computer operating system having a layered plurality of device drivers for accessing data in a data storage device, said first device driver comprising:

15 means for detecting an I/O request to said first device driver;

means for determining whether said first device driver is functionally uppermost in the layered plurality of device drivers;

20 if said first device driver is functionally uppermost in the layered plurality of device drivers, means for performing the I/O request in said first device driver; and

25 if said first device driver is not functionally uppermost in the layered plurality of device drivers, means for denying the I/O request in said first device driver, and means for allowing the I/O request to be performed by a next lower-level device driver in the layered plurality of device drivers.

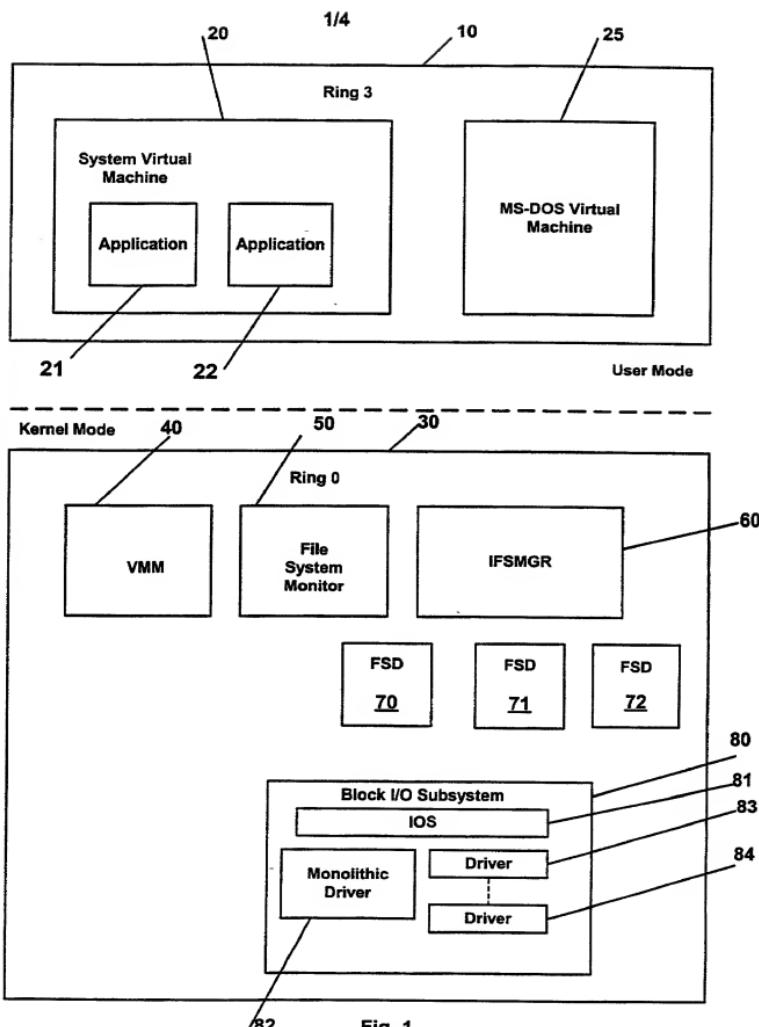


Fig. 1

DRAFT - NOT FOR PUBLICATION

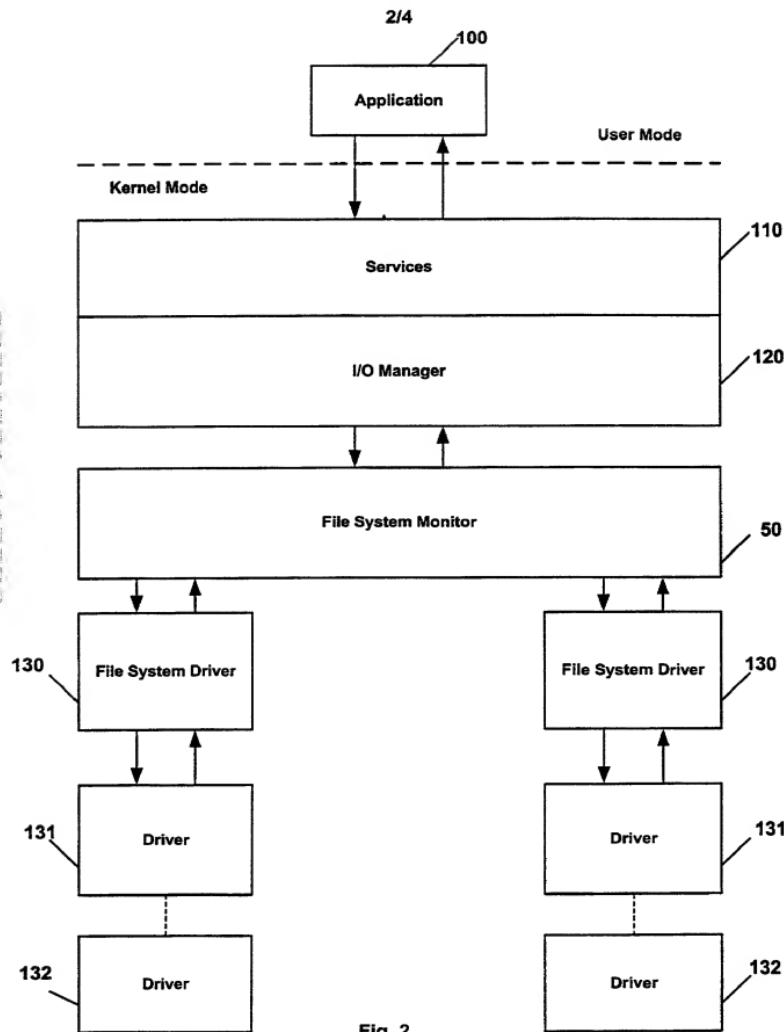


Fig. 2

3/4

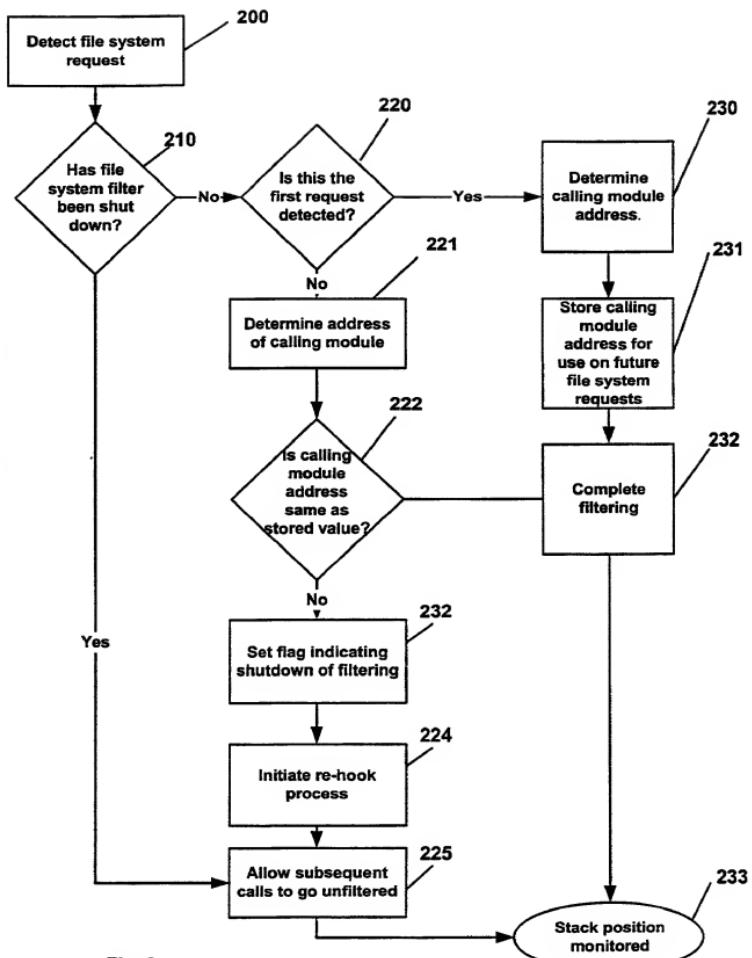


Fig. 3

4/4

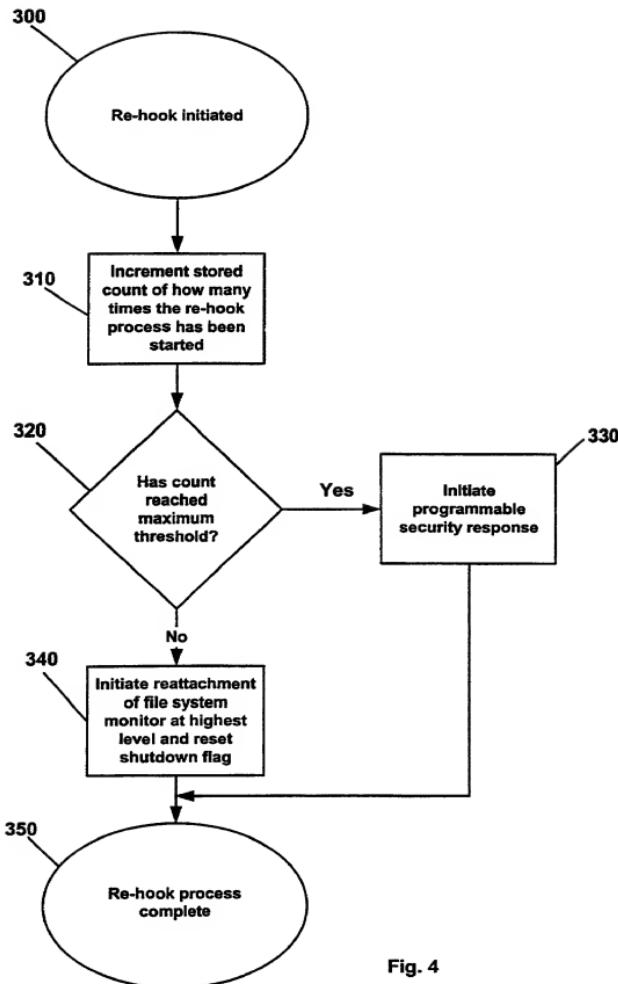


Fig. 4

Declaration and Power of Attorney for Patent Application

As the below named inventor, we hereby declare that:

Our residence, post office address and citizenship are as stated next to our names,

We believe we are the original and first inventors of the subject matter which is claimed and for which a patent is sought on the invention entitled METHOD & SYSTEM FOR PROVIDING DATA SECURITY IN A FILE SYSTEM MONITOR WITH STACK POSITIONING the specification of which is filed herewith.

We hereby state that we have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

We acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

We hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before the application on which priority is claimed:

Prior Foreign Application(s)	Priority Claimed			
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No

We hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, we acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of the application:

PCT/US00/26828 (Application Serial No.)	9/29/00 (Filing Date)	pending (Status) (patent, pending, abandoned)
--	--------------------------	---

We hereby appoint the following attorneys and/or agents to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith:

T. Daniel Christenbury Reg. No. 31,750
Guy T. Donatiello Reg. No. 33,167
Paul A. Taufer Reg. No. 35,703
Austin R. Miller Reg. No. 16,602
James A. Drobile Reg. No. 19,690
Gerard J. Weiser Reg. No. 19,763
Robert A. McKinley Reg. No. 43,793
Michael A. Patané Reg. No. 42,982
Joan T. Kluger Reg. No. 38,940
Sharon Fenick Reg. No. 45,269
Stewart M. Wiener Reg. No. 46,201
Armando A. Flores Reg. No. 41,754
Felicity Rowe Reg. No. 47,042

Address all telephone calls to Paul A. Taufer, Schnader Harrison Segal & Lewis LLP,
Suite 3600, 1600 Market Street, Philadelphia, PA 19103 (215) 751-2475.

Address all correspondence to Paul A. Taufer, Schnader Harrison Segal & Lewis LLP,
Suite 3600, 1600 Market Street, Philadelphia, PA 19103.

We hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under §1001 of Title 18 of the United States Code and that such wilful false statements may jeopardize the validity of the application or any patent issued thereon.

100 Full name of first and joint inventor: George Friedman

Inventor signature George T

11/15/2000

Date

Residence: 7109 Montana Norte, Austin, Texas 78727 TX

Citizenship: USA

Mailing Address: same as above

200 Full name of second and joint inventor: Robert Phillip Starek

Inventor signature Robert P. Starek

11/15/2000

Date

Residence: 1807 W. Slaughter Lane #200-482, Austin, Texas 78748

Citizenship: USA

Mailing Address: same as above

TX

300 Full name of third and joint inventor: Carlos A. Murdock

Inventor signature Carlos A. Murdock

11/15/2000

Date

Residence: 4517 Avenue F, Austin, Texas 78751

Citizenship: USA

Mailing Address: same as above

TX